Roberta Meyer
Associate General Counsel
(202) 624-2184 t (202) 572-4808 f
robbiemeyer@acli.com

January 19, 2007

Via E-Mail

Federal Identity Theft Task Force
c/o Federal Trade Commission
Office of the Secretary
Room H-135 (Annex N)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Federal Identity Theft Task Force

Ladies and Gentlemen:

The American Council of Life Insurers ("ACLI") is pleased to present the views of the life insurance industry to the Federal Identity Theft Task Force (the "Task Force") in connection with its request for public comment on certain issues relating to identity theft. We understand that the Task Force is in the process of developing recommendations on ways to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection and prosecution. ACLI appreciates the opportunity to provide the following comments in connection with this important initiative.

BACKGROUND

ACLI is the principal trade association of life insurance companies whose 373 member companies account for 93 percent of the insurance industry's assets, 91 percent of life insurance premiums and 95 percent of annuity considerations in the United States. ACLI members are also major participants in the pension, long-term care insurance, disability income insurance and reinsurance markets.

Protecting the confidentiality and security of customer information is a critically important matter to life insurers that use this information to provide vital services to our country's consumers. Life insurers' relationships with their customers are personal and confidential. Due to the inherent nature of the life insurance business, ACLI member companies must obtain, maintain, and use sensitive personal information about their policyholders and insureds. As a result, ACLI and its member companies have a significant interest in the Task Force's recommendations.

The life insurance industry has long acknowledged its obligation to maintain and protect the confidentiality and security of customer information and to ensure that it is not compromised or misused by anyone, including identity thieves. The insurance industry expends considerable resources to establish and maintain systems and procedures to protect personal information of customers against a wide range of potential misuse, including threats posed by identity theft. Life insurers recognize that their policyholders and insureds expect them to protect their confidential personal information and they successfully meet that expectation.

In view of the above, ACLI strongly supports the privacy provisions set forth in Title V of the Gramm-Leach-Bliley Act ("GLBA"). We believe the GLBA, the implementing regulations adopted by the federal agencies, and state laws and regulations implementing the GLBA with respect to insurers, appropriately balance consumers' legitimate privacy concerns with their demands for prompt, efficient service and innovative products. These laws and regulations provide clear, comprehensive, and rigorous privacy protections for consumers doing business with insurers and other financial institutions that are not provided customers of virtually any other business. They impose rigorous requirements on life insurers and other financial institutions to protect *both* the confidentiality and the security of their customers' personal information. At the same time, these laws reflect acknowledgment that in order for insurers and other financial institutions to best serve their prospective and existing customers, they must use nonpublic personal information to perform legitimate business functions.

USE OF SOCIAL SECURITY NUMBERS

Because Social Security Numbers ("SSNs") are frequently used to facilitate identity theft, the Task Force indicates that it is exploring ways to achieve reduced reliance on SSNs by federal, state and local governments. In addition, the Task Force is considering whether to recommend that the Task Force investigate and analyze how SSNs are currently used in the private sector, and how these uses could be modified or limited to help minimize the unnecessary exposure of SSNs and to make them less valuable in committing identity theft. Because they are unique, SSNs are used by government agencies and private entities for business and administrative purposes, to detect and deter fraud, identity theft, and other criminal activity, and to comply with federal and state law.

Life insurers must use and responsibly share their customers' personal information, including their SSNs, to perform a host of legitimate, essential insurance business functions – to underwrite applications of prospective customers, to administer and service contracts with existing customers, and to perform related product or service functions. Life insurers also use SSNs to combat and deter fraud and to comply with various federal and state reporting and other legal requirements. Accordingly, ACLI believes it is imperative to avoid restricting necessary and appropriate uses of SSNs by life insurers.

Life insurers do not make SSNs accessible to the general public. Examples of ways in which life insurers use SSNs include the following:

Insurers use SSNs to underwrite applications for new life, disability income, and long term care insurance coverage. SSNs are used in a number of different ways in connection with this process. Insurers sometimes must use proposed insureds' SSNs to obtain medical information from doctors and hospitals that use SSNs as identification numbers; and life insurers use SSNs to ensure they obtain application information about the right person. Life insurers sometimes use motor vehicle record information in underwriting. In some states, insurers are required to use SSNs to obtain this information from the motor vehicle department. Insurers sometimes use information from credit reporting agencies in underwriting; and SSNs are sometimes required to obtain information from consumer reporting agencies.

Once an insurance policy is issued, life insurers use their customers' personal information, including their SSNs, to perform essential, core functions associated with an insurance contract, such as claims evaluations and policy administration. In addition, insurers also use SSNs in connection with the performance of other important business functions related to the administration or servicing of insurance policies generally. The ability to use SSNs for these purposes is crucial to life insurers' ability to meet their contractual obligations to their customers and to perform important related service and administrative functions on a 24/7 basis, in the most cost effective, efficient manner possible. If life insurers are prohibited from using SSNs, or if individuals are permitted to withhold consent or to "opt out" of life insurers' right to use SSNs for these purposes, it would be extremely difficult, if not impossible for insurers to provide the coverage, service, benefits, or economies that otherwise would be available.

SSNs are used by life insurers in connection with the claims process, to obtain information necessary for evaluation of claims. Insurers use SSNs to assure that claims and other payments, such as policy loans and cash surrender payments, are sent to the correct individuals. Life insurers use SSNs to provide 24/7 service to their customers via call centers where insurer representatives use SSNs with other data to authenticate customers requesting various policy services or product or account information or status. SSNs are used by life insurers to find missing or lost beneficiaries to inform them that they are entitled to life insurance proceeds. Life insurers also use SSNs to identify policies owned by an individual who does not have the account or policy number available when a service request is made. SSNs are often needed to transfer assets from an insurer to another financial institution, for example, for transfers between life insurance and annuities or mutual funds. Since one financial institution generally does not know the individual's account number at the other financial institution, the SSN is needed to assure both institutions are dealing with the account of the same person. This reduces delay, error and misplaced assets in such transfers.

Life insurers also use SSNs, along with other personal consumer information, to achieve important public policy goals, most notably, in connection with efforts to detect and deter fraud, identity theft, and other criminal activity. Indeed, SSNs are often integral to life insurers' efforts to protect against illegal activities. Life insurers use personal information, including SSNs, to assist in the detection and prevention of money laundering and terrorist financing activities, as required by the USA Patriot Act and other federal laws. Similarly, insurers use consumers' personal information, including their SSNs, in reporting to state law enforcement agencies and insurance departments to protect against or to prevent actual or potential fraud.

Life insurers use SSNs to fulfill a host of regulatory and legal mandates. They are required to provide SSNs to the Internal Revenue Service ("IRS") and state tax departments in connection with various reporting requirements. Life insurers include SSNs in reports to the IRS regarding a variety of payments to consumers, including, but not limited to, interest payments, certain dividends, and policy withdrawals and surrenders.

As indicated by the above, restrictions on use of SSNs by life insurers could seriously disrupt the ability of insurers to deliver products and services to consumers, as well as interfere with the ability of insurers to detect and deter criminal activity. Limitation of life insurers' ability to obtain information from governmental authorities using SSNs could similarly jeopardize their ability to serve consumers. Moreover, since SSNs are "nonpublic personal information," as defined under the GLBA and implementing state laws and regulations, life insurers already are required to protect *both* the confidentiality and security of SSNs, as required under the privacy provisions of Title V of the GLBA and state laws and regulations, based on the National Association of Insurance Commissioners ("NAIC") Model Privacy of Consumer Financial and Health Information Regulation ("NAIC Model Confidentiality Regulation") and Standards for Safeguarding Customer Information Model Regulation ("NAIC Model Safeguards Regulation"). Unlike virtually all other types of consumers, customers of financial institutions, including life insurers, must be provided annual notice regarding a financial institution's policies for collecting and disclosing their personal information, including their SSNs, and must receive prior notice and the opportunity to "opt-out" of the institution's transfer of the information to nonaffiliated third parties except under certain limited circumstances. Moreover, the security of life insurers' customers' personal information, including their SSNs, must be safeguarded, as explained more fully below.

In view of the above, ACLI strongly believes the Task Force should not recommend further restrictions on the use of SSNs by life insurers.

NATIONAL DATA SECURITY STANDARDS

The Task Force is considering whether to recommend that national data security requirements be imposed on all commercial entities that maintain sensitive consumer information. Title V of the GLBA expresses Congressional policy as to financial institutions' affirmative and continuing obligation to protect the security as well as the confidentiality of their customers' nonpublic personal information. As stated above, ACLI strongly supports the privacy provisions of the GLBA, including those relating to financial institutions' ongoing obligation to protect the security of their customers' information. In fact, life insurers successfully protected the security of their customers' personal information long before they were required to do so by the GLBA or implementing state law. Over the years, life insurers have developed many different ways of ensuring the security of personal consumer information.

Under the GLBA, an institution's primary functional supervisor is required to establish appropriate standards relating to administrative, technical and physical safeguards to:

(i) ensure the security and confidentiality of consumers' nonpublic personal information;
(ii) protect against anticipated threats or hazards to the security or integrity of the information; and
(iii) protect against unauthorized access to, or use of, such records that could result in substantial harm or inconvenience to customers.

The federal agencies with supervisory authority over financial institutions have adopted comprehensive guidance or rules implementing the GLBA's data security provisions. Thirty-four states have adopted comprehensive regulations or statutes that establish standards for safeguarding customer information by insurers. The state requirements all generally track the NAIC Model Safeguards Regulation and are consistent with the federal guidance. Since all insurers, regardless of their state of domicile, are subject to the GLBA, the safeguards outlined in the GLBA and the NAIC Model Safeguards Regulation generally serve as the criteria for security programs of life insurers across the country.

Under state safeguards laws and regulations, life insurers are required to implement a comprehensive written security program that is appropriate to particular insurers' size, and complexity and the nature and scope of their activities. The program must include administrative, technical and physical safeguards for the protection of customer information. It must be designed to: (i) ensure the security and confidentiality of customer information; (ii) protect against any anticipated threats or hazards to the security or integrity of customer information; and (iii) protect against unauthorized access to, or use of, customer information that could result in substantial harm or inconvenience to customers. Insurers also require that companies from which they receive operational services maintain robust information security programs that meet the requirements of the GLBA.

In light of the security protections already afforded personal customer information of the life insurers and other financial institutions, ACLI believes that the Task Force's recommendations relating to national data security standards should take into account that insurers and other financial institutions already have implemented security policies and procedures to protect against identity theft. Duplicative and possibly conflicting new requirements are unlikely to enhance consumer protection.

BREACH NOTICE REQUIREMENTS

The Task Force is considering whether to recommend that a national breach notification requirement be adopted, and what the essential elements of such a national breach notification requirement should be. ACLI supports federal legislation that provides uniform preemptive national standards for notification to individuals whose personal information has been subject to a security breach. It is of utmost importance to ACLI member companies that the substantive provisions of any federal security breach notification legislation clearly and completely preempt any state laws relating to investigation and notification of security breaches.

ACLI strongly supports a uniform preemptive national standard to address the myriad state laws that have resulted in a patchwork of breach notification laws. More than thirty states have enacted legislation requiring companies to notify consumers in the event their sensitive personal information is affected by a security breach of company information systems. These statutes typically require disclosure of a breach of security to the person whose unencrypted sensitive information was or is reasonably believed to have been compromised.

The state laws differ in certain key respects. While most of the state laws require notice in connection with breaches in the security of computerized information only, others extend to breaches in the security of any consumer information – paper or computerized information. Some of the states' triggers for notice are tied to the likelihood of harm to consumers; others are not. Some require delay in notice at the request of law enforcement; others do not. The state laws also have different enforcement mechanisms. Many are enforced by state attorneys general, a few by state insurance commissioners with respect to insurers; and some laws provide for private rights of action for violations.

The differences in these laws are likely to result in different notification to consumers in different states. Also, the need to track the differences in the various states' laws and to factor them into a notification program makes it more difficult for institutions to send notices to consumers promptly. Moreover, differing state laws will result in different and possibly overlapping enforcement mechanisms, which increases the likelihood of uneven enforcement from state to state.

If the substantive requirements for investigation and notice of security breaches are the same regardless of where a consumer lives or the type of entity subject to the breach, consumers will be provided clear, consistent protection across the country. In view of the above, ACLI urges the Task Force to recommend federal legislation that provides uniform preemptive substantive standards for notification to individuals whose personal information has been subject to a security breach.

ACLI believes that it also is critically important that the enforcement of life insurers' compliance with any preemptive substantive standards for investigation and notice of security breaches be as uniform as possible. For this reason, ACLI strongly supports enforcement of insurers' compliance with federal security breach notification legislation exclusively by the Department of the Treasury.

The Treasury Department has extensive experience working with the insurance industry in connection with the implementation and enforcement of laws such as the USA Patriot Act, the Terrorism Risk Insurance Act and the Bank Secrecy Act, as well as regulations promulgated by the Office of Foreign Asset Control. As a result of this extensive experience, ACLI believes that the Treasury is well-positioned to implement and enforce the insurance industry's compliance with security breach investigation and notification requirements.

Uniform enforcement of the substantive security breach investigation and notice requirements is also necessary to ensure even-handed consumer protection across the country. Accordingly, ACLI urges the Task Force to support enforcement of insurers' compliance with preemptive substantive security breach investigation and notice requirements exclusively by the Department of the Treasury.

ACLI also supports legislation that avoids needlessly alarming individuals and undermining the significance of notification by requiring notification only when the security and confidentiality of personal information is truly at risk of identity theft. Accordingly, the ACLI supports legislation that does not require notification if personal information is protected by encryption or some other means that makes the information unreadable or unusable, or if the formation is not otherwise likely to be subject to identity theft.

Accordingly, ACLI believes that if the Task Force recommends enactment of a uniform preemptive national standard for investigation and notification of security breaches, it should ensure that notification of a breach is required to be provided to consumers only when the security and confidentiality of sensitive personal information, such as a person's name and address, when combined with information such as account number or SSN, is truly at risk of identity theft. Moreover, notification should not be necessary if sensitive personal information is protected by encryption or some other means that makes the information unreadable or unusable, or if the information is not otherwise likely to be used in connection with identity theft.

CONSUMER EDUCATION

The Task Force is considering whether there is a need to better educate consumers on how to safeguard their personal data and how to detect and deter identity theft, through a national public awareness campaign. ACLI believes that such education campaigns can be an effective way in which to address the problem of identity theft. Such programs should inform the public about measures they can follow to protect themselves against identity theft.

CONCLUSION

The issues before the Task Force are complex and should be carefully studied, as you are doing. ACLI anticipates that recommendations the Task Force presents will provide meaningful protections to consumers who might otherwise become victims of identity theft. The ACLI appreciates the opportunity to provide its comments to the Task Force.

Sincerely,

Roberta B. Meyer